UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/590,415	10/20/2006	Nicolas Popp	028572-003210US	7016

20350 7590 02/15/2011
KILPATRICK TOWNSEND & STOCKTON LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
NIGH, JAMES D	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
02/15/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Docket@kilpatricktownsend.com
ipefiling@kilpatricktownsend.com
jlhice@kilpatrick.foundationip.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/590,415
Filing Date: October 20, 2006
Appellant(s): POPP, NICOLAS

Aaron S Kamlay
Reg. No 58,813
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 13 December 2010 appealing from the Office action mailed 13 October 2010.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The following is a list of claims that are rejected and pending in the application:

Claims 1-11

(4) Status of Amendments After Final

The examiner has no comment on the appellant's statement of the status of amendments after final rejection contained in the brief.

(5) Summary of Claimed Subject Matter

The examiner has no comment on the summary of claimed subject matter contained in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

The examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal. Every ground of rejection set forth in the Office action from which the appeal is taken (as modified by any advisory actions) is being maintained by the examiner except for the grounds of rejection (if any) listed under the subheading “WITHDRAWN REJECTIONS.” New grounds of rejection (if any) are provided under the subheading “NEW GROUNDS OF REJECTION.”

(7) Claims Appendix

The examiner has no comment on the copy of the appealed claims contained in the Appendix to the appellant’s brief.

(8) Evidence Relied Upon

5,953,420	Matyas, Jr. et al.	09-1999
2003/0172269	Newcombe	09-2003

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Response to Arguments

1. Applicant’s argument with regard to the 35 U.S.C. § 101 rejection of claims 1-9 has been fully considered and is persuasive. Accordingly the rejection will be withdrawn.

2. Applicant’s argument with regard to the 35 U.S.C. § 103 (a) rejection of claims 1-9 has been fully considered but is not persuasive.

Prior to addressing Applicant’s argument, Examiner is producing a definition of the word “token” from the Microsoft Computer dictionary:

> token n. 1. A unique structured data object or message that circulates continuously among the nodes of a token ring and describes the current state of the network. Before any node can send a message, it must first wait to control the token. See also token bus network, token passing, token ring network. 2. Any nonreducible textual element in data that is being parsed—for example, the use in a program of a variable name, a reserved word, or an operator. Storing tokens as short codes shortens program files and speeds execution.

As such nothing within Applicant's claims excludes a software "token". The language in fact is simply a recitation of non-functional descriptive material as the recitation regarding how the one-time passwords are generated is not part of the claimed method steps. As such it is not entitled to patentable weight, and therefore cannot be used to distinguish the claimed invention from the prior art.

With regard to claim interpretation, per MPEP § 2173.02 regarding "clarity and precision": "Some latitude in the manner of expression and the aptness of terms should be permitted even though the claim language is not as precise as the examiner might desire"; in addition per MPEP § 2173.04 "breadth is not indefiniteness".

Also with regard to the interpretation of words of a claim will be given their "plain meaning" unless such meaning is inconsistent with the specification (MPEP § 2111.01) "Although claims of issued patents are interpreted in light of the specification, prosecution history, prior art and other claims, this is not the mode of claim interpretation to be applied during examination. During examination, the claims must be interpreted as broadly as their terms reasonably allow. *In re American Academy of Science Tech Center*, 367 F.3d 1359, 1369, 70 USPQ2d 1827, 1834 (Fed. Cir. 2004).

Applicant's disclosure regarding the word token (page 1, line 30 "A token is a device that can be used to authenticate a user"; page 2, lines 22-26 "An embodiment of the present invention includes a protocol for generating One Time Passwords ("OTPs") at a hardware device that can be used to authenticate a user. The OTPs are generated by a token, '*which can be a physical device'* that includes mechanisms to prevent the unauthorized modification or disclosure of the software and information that it contains, and to help ensure its proper functioning.) only recites what a token could be, but recites no explicit definition of what it is. Furthermore the original claims as recited did not incorporate into the claims limiting language that would have placed the traditional Microsoft Computer Dictionary definition of a token outside the broadest reasonable interpretation.

As claims 1 and 6 are directed towards a method and not an apparatus, if arguably the token were to be interpreted as structure the recitation of structure (in this case Applicant's "token") must manipulatively affect the method in order to receive patentable weight "As to the rejection of the claims on the prior art references, we do not agree with the appellant that such structural limitations as are not disclosed by the references should be given patentable weight. This argument is applicable to claims drawn to structure and not claims drawn to a method. To be entitled to such weight in method claims, the recited structural limitations therein must affect the method in a manipulative sense and not to amount to the mere claiming of a use of a particular structure, which, in our opinion, is the case here", *Ex parte Pfeiffer*, 135 USPQ 31 (BdPatApp&Int 1961). Such is not the case with claims 1 and 6, particularly in light of the fact per Applicant's disclosure the only relevant teaching regarding the structure is that a token "can be a physical device". Moreover Examiner does not agree that with

Applicant "a ticket is not similar to a token" as per the Microsoft computer dictionary a token is a data structure. Thus Examiner sees Applicant's remarks as providing evidence that the Applicant within the originally presented claims did not, as required by 35 U.S.C. § 112, 2nd paragraph, "set forth the subject matter that applicants regard as their invention" (See MPEP § 2171, also MPEP § 2172 II "Evidence that shows that a claim does not correspond in scope with that which applicant regards as applicant's invention may be found, for example, in contentions or admissions contained in briefs or remarks filed by applicant, *Solomon v. Kimberly-Clark Corp.*, 216 F.3d 1372, 55 USPQ2d 1279 (Fed. Cir. 2000); *In re Prater*, 415 F.2d 1393, 162 USPQ 541 (CCPA 1969).

Moreover as the recitation of claim 1 "where the secret is uniquely assigned to a token and is shared between the token and an authentication server, and the count is a number that increases monotonically at the token with the number of One Time Passwords generated by the token and increases monotonically at the authentication server with each calculation by the authentication server of a One Time Password" is simply non-functional descriptive material as it merely describes the secret and count without reciting method steps; again the recitation is not entitled to patentable weight. See MPEP § 2106 II C and 2111.04.

As the cited Matyas reference discloses "workstations" (4:24-36) that generate the count and shared secret value to form the concatenated value (5:17-25), the Matyas reference meets Applicant's definition of a "token" as a workstation is a physical device. Newcombe in paragraphs 0058 and 0064-0066 teaches that the shared ticket is shared between a server and a client device (again physical devices). Therefore even in light of Applicant's remarks the combination of Matyas and Newcombe teaches claim 1.

3. Applicant's argument with regard to claim 2 regarding the recitation "if the calculated..." has been fully considered but is not persuasive. The recitation is directed to optional language which is not limiting "Language that suggests or makes optional but does not require steps to be performed or does not limit a claim to a particular structure does not limit the scope of a claim or claim limitation", MPEP § 2106 II C.

4. Applicant's argument with regard to claim 2 regarding a token based upon a serial number or user name has been fully considered but is not persuasive. Applicant's argument is only directed at the Matyas reference when a combination of Newcombe was provided. In response to applicant's arguments against the Matyas reference individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

5. Applicant's argument that the next action should be made non-final has been fully considered but is not persuasive. Applicant, as evidenced by remarks, failed in the originally presented claims to set forth the subject matter as required by 35 U.S.C. § 112, 2nd paragraph; in addition the Applicant is placing reliance on recitations not entitled to patentable weight and optional language. Moreover Applicant has attacked reference individually instead of in combination. Examiner also maintains that the cited

combination of Matyas and Newcombe teach invention as claimed. Therefore this action will be made final.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 1-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas Jr. et al. (U.S. Patent 5,953,420, hereinafter referred to as Matyas) in view of Newcombe (U.S. Patent PG Publication 2003/0172269, now U.S. Patent 7,392,390, hereinafter referred to as Newcombe).**

8. As per claim 1

Matyas explicitly discloses concatenating a secret with a count (Abstract, 2:29-49, 5:17-31, 5:39-59)

Matyas explicitly discloses the count number that increases monotonically (Figure 4, 5:17-25)

Matyas explicitly discloses the count number that increases monotonically with the number of One Time Passwords generated and increases monotonically at the authentication server with each calculation at the authentication server of a One Time Password (Figure 4, 5:17-25)

Matyas explicitly discloses hashing and truncating the result (5:26-31, 5:60-64)

Matyas discloses a token (4:24-36)

Matyas does not explicitly disclose where the secret is uniquely assigned to token and is shared between the token and an authentication server.

Newcombe teaches where the secret is uniquely assigned to token and is shared between the token and an authentication server. (0051, 0058, 0064-0066, 0068, 0072, 0091)

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the method for establishing an authenticated shared secret value between a pair of users of Matyas with the method for binding Kerberos style authenticators to single clients of Newcombe for the purpose of enabling improved authentication in a distributed environment.

"where the secret is uniquely assigned to a token and is shared between the token and an authentication server, and the count is a number that increases monotonically at the token with the number of One Time Passwords generated by the token and increases monotonically at the authentication server with each calculation by the authentication server of a One Time Password" is simply non-functional descriptive material "Where the printed matter is not functionally related to the substrate, the printed matter will not distinguish the invention from the prior art in terms of patentability .... [T]he critical question is whether there exists any new and unobvious functional relationship between the printed matter and the substrate" *In re Gulack*, 217 USPQ 401 (Fed. Cir. 1983), *In re Ngai*, 70 USPQ2d (Fed. Cir. 2004), *In re Lowry*, 32 USPQ2d 1031 (Fed. Cir. 1994); MPEP 2106.01 II

9. As per claim 2

Matyas explicitly discloses receiving a request for authentication (2:35-57, 5:1-10, 5:46-59, 7:25-37)

Matyas explicitly discloses concatenating a secret with a count (Abstract, 2:29-49, 5:17-31, 5:39-59)

Matyas explicitly discloses calculating the one time password based on count values and the secret (Figure 4, 5:17-25)

Matyas explicitly discloses a token (4:24-46)

Matyas explicitly discloses incrementing the count (5:46-59)

Matyas explicitly discloses retrieving a count (5:46-59)

Matyas explicitly discloses retrieving a secret (6:62-65)

Matyas explicitly discloses calculating a one-time password based upon retrieved values of the count and the secret corresponding to the token (4:24-46, 5:17-30, 5:46-59)

Matyas explicitly discloses comparing the calculated one time password with the received one time password (6:45-61)

Matyas explicitly discloses that if the calculated and received password match that the request is authenticated (6:45-61).

Matyas, while disclosing authentication, does not explicitly disclose an authentication server or serial numbers

Newcombe teaches a serial number uniquely associated with a token (IP address, 0025, 0048, 0051)

Newcombe teaches a personal identification number associated with a user (password, 0057-58, 0065-0067)

Newcombe teaches an authentication server (0047, 0057)

Newcombe teaches where the secret is retrieved by the authentication server based upon the serial number (0025, 0040-0041)

Matyas while disclosing a count does not explicitly disclose recalculating, Newcombe does not explicitly teach incrementing the count and recalculating; however Newcombe teaches a window of acceptable values for time with which recalculation can occur and authenticate the client (0059, 0068, 0070, 0097). Thus a predictable result (*KSR International Co. v. Teleflex Inc.,* 82 USPQ2d 1385 (U.S. 2007)) of Matyas and Newcombe would be to substitute the count value for the time value, perform the incrementing of the count and recalculate to determine if the count was acceptable for the purpose of enabling improved authentication in a distributed environment.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the method for establishing an authenticated shared secret value between a pair of users of Matyas with the method for binding Kerberos style authenticators to single clients of Newcombe for the purpose of enabling improved authentication in a distributed environment.

However the recitations beginning with the word "if" are merely reciting optional language these are not-limiting and are not entitled to patentable weight MPEP § 2106 II C.

10. As per claims 3 and 7

Newcombe teaches an SHA-1 hash function (0029-0030, 0068, 0103)

11. As per claims 4 and 8

Newcombe teaches a symmetric key (0028, 0032).

12. As per claims 5 and 9

Newcombe teaches “an acceptable time window” which would encompass a predetermined number of times for authentication (0059, 0068, 0070, 0097).

13. As per claim 6

Matyas explicitly discloses receiving a request for authentication (2:35-57, 5:1-10, 5:46-59, 7:25-37)

Matyas explicitly discloses concatenating a secret with a count (Abstract, 2:29-49, 5:17-31, 5:39-59)

Matyas explicitly discloses calculating the one time password based on count values and the secret (Figure 4, 5:17-25)

Matyas explicitly discloses retrieving a count based on a username (certificate and public value) (4:47-67, 5:46-59, 6:22-65)

Matyas explicitly discloses retrieving a secret based on a user name (6:22-65)

Matyas explicitly discloses comparing the calculated one time password with the received one time password (6:45-61)

Matyas explicitly discloses that if the calculated and received password match that the request is authenticated (6:45-61).

Matyas, while disclosing authentication and users does not explicitly disclose personal identification numbers. Newcombe teaches a personal identification number associated with a user (password, 0057-58, 0065-0067)

Matyas while disclosing a count does not explicitly disclose recalculating, whereas Newcombe does not explicitly teach incrementing the count and recalculating; However Newcombe teaches a window of acceptable values for time with which recalculation can occur and authenticate the client (0059, 0068, 0070, 0097). Thus a predictable result (*KSR International Co. v. Teleflex Inc.,* 82 USPQ2d 1385 (U.S. 2007)) of Matyas and Newcombe would be to substitute the count value for the time value, perform the incrementing of the count and recalculate to determine if the count was acceptable for the purpose of enabling improved authentication in a distributed environment.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the method for establishing an authenticated shared secret value between a pair of users of Matyas with the method for binding Kerberos style authenticators to single clients of Newcombe for the purpose of enabling improved authentication in a distributed environment.

However as the recitations beginning with the word "if" are merely reciting optional language these are not-limiting and are not entitled to patentable weight MPEP § 2106 II C.

14. As per claims 10 and 11 Matyas discloses wherein the secret is uniquely assigned to the token (4:24-36, 5:17-25, 46-59); however this recitation is simply non-functional descriptive material.

(10) Response to Argument

Appellants argument that "The Final Office Action Fails to Show that the Cited References Disclose or Suggest a "Token". Examiner begins by reciting claim 1 in its entirety:

Claim 1. A method for calculating a One Time Password, comprising:

concatenating, by a computer, a secret with a count, where the secret is uniquely assigned to a token and is shared between the token and an authentication server, and the count is a number that increases monotonically at the token with the number of One Time Passwords generated by the token and increases monotonically at the authentication server with each calculation by the authentication server of a One Time Password;

calculating, by a computer, a hash based upon the concatenated secret and count; and

truncating the result of the hash to obtain a One Time Password.

It should be pointed out that much of the language in that is brought in Appellant's argument is not being positively recited in the form of method steps. For example the recitation "where the secret is uniquely assigned to a token and is shared between the token and an authentication server" does not positively recite that the secret is assigned to a token as part of the method performed by the computer but instead is only offered as descriptive material regarding the secret. As such this action may not necessarily be part of the claimed method as it is only presented in the form of a "suggested" method step which is not limiting per MPEP § 2106 II C. Similarly the recitation "the count is a number that increases monotonically at the token with the number of One Time Passwords generated by the token and increases monotonically at the authentication server with each calculation by the authentication server of a One Time Password" does not positively recite that the count is being increased as part of the method but again is only offered as descriptive material regarding the count and similarly would not be limiting per MPEP § 2106 II C. As the recited particular machine actually performing the method steps of concatenating and calculating is simply a general purpose computer and is the only structure positively recited as performing steps within the claim it becomes clear that the only structure that is relevant to the claimed invention is the general purpose computer. As such it is apparent that the claimed invention is not manipulatively affected by the source of either the secret or the count. While the secret and the count could be generated either by the general purpose computer recited in the claims or externally from the general purpose computer the method steps as recited do not dictate any structure other than the claimed computer. It should also be pointed out that the disclosure does not teach that the token contains any type of computer or processor and the computer that is recited in the claim cannot be construed as having any structural association with the token for that reason. The recitation “a token is a device…" in paragraph 0004 without any subsequent structural description does not necessarily place the recited token in the physical realm, particularly in light of the recitation of paragraph 0007 "The OTPs are generated by a token, which _can_ be a physical device…” which indicates that a physical device is optional. The word “device” itself can be an abstraction:

> ▨ **device** *n* -S **c** : something in a literary work designed to achieve a particular artistic effect (as a figure of speech, a special method of narration, or use of words or word sounds)

The absence of any recitation regarding within the disclosure regarding any physical properties of the token suggests that the token could be a separate physical device but also in the broadest reasonable interpretation in light of the specification simply a software routine being performed on a general purpose computer or even as claimed simply an abstraction.

Therefore with regard to claim 1 the prior art need only teach a computer concatenating a secret with a count and then calculating a hash based on the concatenated secret and count and then truncating the hash. Matyas discloses concatenating a secret with a count (Abstract, 2:29-49, 5:17-31, 5:39-59, Matyas explicitly discloses hashing the concatenated secret and count (5:26-31) and Matyas explicitly discloses truncating the result (5:60-64)

However with regard to the disputed token, the recited workstations of Matyas (4:24-36) which perform the operations regarding the count (5:11-25) and the One Time

Passwords that are generated (4:24-46, 5:17-30, 5:46-59) cannot be excluded as Appellant suggests as nothing within the recited claim or the disclosure excludes such an interpretation. The token in this instance can be viewed as the "suitable combination of hardware and/or software" (4:29-30) within the workstation disclosed by Matyas. As such the "token" would constitute a virtual device operating within the physical workstation performing the functions of the token as recited. A secret is uniquely assigned to the token (5:1-16) which is shared between the token and the authentication server (which in this case would comprise the other user. The virtual token of user A would be viewed as having its secret shared with user B which in effect becomes the authentication server for user A; similarly the virtual token of user B would be viewed as having its secret shared with user A which becomes the authentication server for user B using Matyas' example, 4:37-46, 6:2-7).

Therefore with regard to Appellant's argument that "the cited references do not disclose the recited token", Examiner would maintain that what is disclosed by Matyas is a token operating as a virtual device within the workstation disclosed by Matyas per the above line of reasoning.

Appellant's argument that the "Office Action Fails to Show that the Cited References disclose of Suggest a Secret that is Uniquely Assigned to a Token" ha been fully considered but is not persuasive. Examiner would maintain that when the token is viewed as a virtual device operating within the workstation disclosed by Matyas that the secret disclosed by Matyas (5:1-16) must be viewed as being uniquely assigned to that token as it is unique to each user's workstation ("user A generates a dynamic value Z2a (414), while user B generates an identical dynamic value Z2b (416)").

Appellant's argument with regard to claims 2 and 6 that "The Final Office Action Fails to Show that the Cited References Disclose or Suggest that if the Calculated One Time Password Does Not Correspond to the Received One Time Password, then Incrementing the Count and Recalculating the One Time Password" has been fully considered but is not persuasive. As pointed out the language is optional in nature and is not limiting per MPEP § 2106 II C. Matyas explicitly discloses that if the calculated and received password match that the request is authenticated (6:45-61). Thus if the passwords match the other conditional language will not be performed. "As matter of linguistic precision, optional claim elements do not narrow claim, since they can always be omitted; in present case, elements of dependent claim directed to large diameter spirally formed pipe, which recite "further including that said wall may be smooth, corrugated, or profiled with increased dimensional proportions as pipe size is increased," do not narrow scope of claim compared to claims lacking those elements, since elements are stated in permissive form "may". *In re Johnston*, 77 USPQ2d 1788 (CA FC 2006), "Because the language of claim 1 refers to "programmable selection means" and states "whereby when said alternate addressing mode is selected" (emphases added), the accused device, to be infringing, need only be capable of operating in the page mode. Contrary to GI/M's argument, actual page mode operation in the accused device is not required", *Intel Corp. v. Int'l Trade Comm'n*, 20 USPQ2d 1161 (Fed. Cir. 1991), "It has been held that actions that may or may not be done are indefinite and does not distinguish the claim from the prior art", *In re Collier*, 158 USPQ 266 (CCPA 1968). Furthermore Appellant is attacking the Newcombe reference for the portion regarding the count when this was disclosed by the Matyas reference. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Appellant's argument that " Claims 2-11: The Office Action Fails to Show that the Cited References Disclose or Suggest Retrieving the Value of a Count that Corresponds to a Token Based Upon a Serial Number or a User Name" has been fully considered but is not persuasive. When considering that Matyas in essence discloses a virtual token then the IP address taught by Newcombe would be a serial number that would be unique to each workstation's virtual token device. Newcombe teaches where the secret is retrieved by the authentication server based upon the serial number (0025, 0040-0041), and that the IP address is used as part of the validation (0119-0120) which would serve as the "basis" for subsequent action.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/JAMES D NIGH/
Examiner, Art Unit 3685

/Calvin L Hewitt II/
Supervisory Patent Examiner, Art Unit 3685

<u>Conferees</u>:

Calvin L Hewitt II/C.L.H./
Supervisory Patent Examiner, Art Unit 3685

Andrew J. Fischer /A. J. F./
Supervisory Patent Examiner, Art Unit 3621